Basic Axioms and Examples

Note 1

cca4f1927b2c4eeaa3123dbcf0680bc0

Given a set G, {{c2::a binary operation $\star$ on G}} is {{c1::a function

$$\star : G \times G \to G.$$

}}

Note 2

7732d25ebb1e40dd9696c1c921803c17

Given a binary operation $\star$ on a set G, for any $a, b \in G$ we shall write {{c2::$a \star b$}} for {{c1::$\star(a, b)$.}}

Note 3

4fc60827250f4af4ab6a669ac7632568

A binary operation $\star$ on a set G is {{c2::associative}} if {{c1::for all $a, b, c \in G$ we have

$$a \star (b \star c) = (a \star b) \star c.$$

}}

Note 4

192d8d86f22349cabcd9f4229fc45290

If $\star$ is a binary operation on a set G we say elements a and b of G {{c1::commute}} if {{c2::

$$a \star b = b \star a.$$

}}

Note 5

e5cbf512d6a54c91950c65450a07a501

A binary operation $\star$ on a set G is {{c2::commutative}} if {{c1::for all $a, b \in G$ we have

$$a \star b = b \star a.$$

}}

Note 6

36b096eebd7f4264ab071a5fa4eefe13

Suppose that $\star$ is a binary operation on a set G and $H \subseteq G$. If {{c2::the restriction of $\star$ to H is a binary operation on H,}} then H is said to be {{c1::closed under $\star$.}}

Note 7

644b1cd8fa014885ad295ae5c089e5a7

{{c3::A group}} is {{c2::an ordered pair $(G, \star)$}} where {{c1::G is a set and $\star$ is a binary operation on G}} satisfying {{c4::the group axioms.}}

Note 8

5de4e717b4814adf8aed4f8d9a93322c

How many axiom are there in the definition of a group $(G, \star)$?

> Three.

Note 9

2de690f5008a4b8c8691e36308e44295

What is the first axiom from the definition of a group $(G, \star)$?

> $\star$ is associative.

Note 10

4fcc137e66a048459cc73d6735e4ccea

Given a binary operation $\star$ on a set G, {{c3::an element $e \in G$}} is called {{c2::an identity of G}} if {{c1::for all $a \in G$ we have

$$a \star e = e \star a = a.$$

}}

Note 11

a3cd125f152f432082757242096a76ef

What is the second axiom from the definition of a group $(G, \star)$?

> There exists an identity of G.

Note 12

5d438f0c3fb24b1a97507e81f868846e

Given a binary operation $\star$ on a set G and $a \in G$, {{c3::an element $\tilde{a} \in G$}} is called {{c2::an inverse of a}} if {{c1::

$$a \star \tilde{a} = \tilde{a} \star a = e.$$

}}

Note 13

d840b7b910d740f3bea231c74feba51c

Given a binary operation $\star$ on a set G and $a \in G$, {{c2::an inverse of a}} is usually denoted {{c1::a^{-1}.}}

Note 14

c4c56a11c6f746b3ae287ee386b4e12b

What is the third axiom from the definition of a group $(G, \star)$?

> For all $a \in G$ there exists a^{-1}.

Note 15

be05e23d350d4f49a65602b65045f888

A group $(G, \star)$ is called {{c2::abelian}} if {{c1::$\star$ is commutative.}}

Note 16

978f23382d594a28a3de168b7f661c30

We shall say G is {{c2::a group under $\star$}} if {{c1::$(G, \star)$ is a group.}}

Note 17

497f01593d7f4ffabb546b455788b354

We shall say a set G is {{c2::a group}} if {{c1::G is a group under an operation that is clear from the context.}}

Note 18

61ea2504ca474fe4aae902eb1965576c

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are {{c2::groups}} under {{c1::$+$.}}

Note 19

84b6a231d3934ab3b4f63226549a9589

$\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$ are {{c2::groups}} under {{c1::$\times$.}}

Note 20

3051cd354f5040e2bdf0809e005635ed

$\mathbb{Q}^+, \mathbb{R}^+$ are {{c2::groups}} under {{c1::$\times$.}}

Note 21

21f924e833cd4e0bbae5f4588dff47b5

Is $\mathbb{Z} - \{0\}$ a group under $\times$?

> No. (There is no inverse.)

Note 22

edec2a960f6d43dbb5e19283c28db7bd

Let V be a vector space. Then V is {{c2::a group}} under {{c1::$+$.}}

Note 23

47a03e2c688244b1b3a5126fd04a21c7

Let $n \in \mathbb{Z}^+$. Then {{c3::$\mathbb{Z}/n\mathbb{Z}$}} is {{c2::a group}} under {{c1::addition}} of residue classes.

Note 24

f6a5a40cfee6495dae0d36f7b3288cb2

Let $n \in \mathbb{Z}^+$. Then {{c3::$(\mathbb{Z}/n\mathbb{Z})^\times$}} is {{c2::a group}} under {{c1::multiplication }} of residue classes.

Note 25

3e94ca73ca344269bb98d94a22204fd9

If $(A, \star)$ and $(B, \diamond)$ are {{c4::groups,}} then the group {{c2::$A \times B$,}} whose operation is {{c1::defined componentwise:

$$(a, b)(c, d) = (a \star c, b \diamond d),$$

}} is called {{c3::the direct product of the two groups.}}

Note 26

e23d8e577b3948af9b0cadd5df7c9141

If $(G, \star)$ is a group, then {{c2::the identity of G}} is {{c1::unique.}}

Note 27

5b5391986e9b49ea9c5f9f73813e9594

If $(G, \star)$ is a group, then the identity of G is unique. What is the key idea in the proof?

> Consider the product of two arbitrary identities.

Note 28

0989a259fae446c48bb0f6c40394efd0

If $(G, \star)$ is a group, then for every $a \in G$, {{c2::a^{-1}}} is {{c1::uniquely determined.}}

Note 29

f0b0a651592c466ba8067beb3b1570b8

If $(G, \star)$ is a group, then for every $a \in G$, a^{-1} is uniquely determined. What is the key idea in the proof?

> Multiply an inverse on the right by $a \star a^{-1}$.

Note 30

4a6a6806d8874839bb7956d76e384333

If $(G, \star)$ is a group and $a \in G$, then

$$(a^{-1})^{-1} = \text{\{\{c1::}a.\text{\}\}}$$

Note 31

9ab0e972d6a24baea99f1577ebf03423

If $(G, \star)$ is a group and $a, b \in G$, then

$$\text{\{\{c2::}(a \star b)^{-1}\text{\}\}} = \text{\{\{c1::}(b^{-1}) \star (a^{-1}).\text{\}\}}$$

Note 32

69b3db6e70ad4629aa55a855b8df8096

If $(G, \star)$ is a group and $a_1, \ldots, a_n \in G$, then the value of

$$a_1 \star \cdots \star a_n$$

is {{c2::independent}} of {{c1::how the expression is bracketed.}}

«{{c3::The generalized associative law}}»

Note 33

05cc8fd523084650adb46704dde222a7

What is the key idea in the proof of the generalized associative law for a group $(G, \star)$?

> By induction.

Note 34

9ca193d1531c4c49b296732d7ff12fb5

Henceforth our abstract groups G, H, *etc.* will always be written with the operation as {{c1::$\cdot$.}}

Note 35

7d06acac21c14a628ad1ccb470fe6398

Henceforth for an abstract group G (operation $\cdot$) an expression {{c2::$a \cdot b$}} will always be written as {{c1::ab.}}

Note 36

0994e6080f3042ad81bc90d1ced0b747

Henceforth for an abstract group G (operation $\cdot$) we denote {{c2:: the identity of G}} by {{c1::1.}}

Note 37

361c99f13a9b4304868fcdb350b45dbf

For any group G and $x \in G$ and {{c3::$n \in \mathbb{Z}^+$}} we shall denote by {{c2::x^n}} {{c1::the product

$$\underbrace{xx \cdots x}_{n \text{ terms}}.$$

}}

Note 38

5b7f3c41cf0147e2bffc3929ed9ec480

For any group G and $x \in G$ and {{c3::$n \in \mathbb{Z}^+$}} we shall denote by {{c2::x^{-n}}} {{c1::the product

$$\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}}.$$

}}

Note 39

a7a44229ee0f4a44b11d1410dc0fab0f

For any group G and {{c3::$x \in G$,}} let $x^{\{\{c2::0\}\}} \stackrel{\text{def}}{=}$ {{c1::1, the identity of G}}.

Note 40

b1be1b97f53c45fa9451eaa7112ca406

Let G be a group and let $a, u, v \in G$. Then $au = av$ {{c2::if and only if}} {{c1::$u = v$.}}

«{{c3::Cancellation rule}}»

Note 41

ed8673154d544c7b86ac358facc79101

For G a group and $x \in G$ define {{c2::the order of x}} to be {{c1::the smallest positive integer n such that

$$x^n = 1.$$

}}

Note 42

8c334a6360be4bee8fae7f712ab2c4ee

For G a group and $x \in G$, if {{c2::no positive power of x is the identity,}} {{c3::the order of x}} is defined to be {{c1::infinity.}}

Note 43

ba4143a322564f8383f6e7d91ca32a75

For G a group and $x \in G$, denote {{c2::the order of x}} by {{c1::$|x|$.}}

Note 44

d7fee5bcbdbd47bcb6f4a2ba086fa2ed

For G a group and $x \in G$, if {{c2::the order of x is an integer n,}} x is said to be {{c1::of order n.}}

Note 45

db12c606699d40e89d499d554bd52b28

For G a group and $x \in G$, if {{c2::the order of x is infinite,}} x is said to be {{c1::of infinite order.}}

Note 46

2e514c62ce4e48eb9c6bd3b5de1d7c44

An element of a group has order 1 {{c2::if and only if}} {{c1::it is the identity.}}

Note 47

babeb7cf1b394be6a4f8d86e1a099cda

Let $G = \{g_1, g_2, \ldots, g_n\}$ be {{c4::a finite group}} with {{c3::$g_1 = 1$.}} The {{c2::multiplication table}} or {{c2::group table}} of G is {{c1::the matrix

$$\left[g_i g_j\right] \sim n \times n.$$

}}

Note 48

f245736b42b44f178f9a1d661bc4a5c7

Let $G =$ {{c3:: $\{x \in \mathbb{R} \mid x \in [0, 1)\}$ }} and for $x, y \in G$ let $x \star y$ be {{c2:: the fractional part of $x + y$.}} Then the group {{c4::$(G, \star)$}} is called {{c1::the real numbers mod 1.}}

Note 49

3664191737c844f38816547b7acd64c1

Let $G = \{z \in$ {{c3::$\mathbb{C}$}} $\mid$ {{c2::$z^n = 1$ for some $n \in \mathbb{Z}^+$}}$\}$. Then the group $(G, +)$ is called {{c1::the group of roots of unity in $\mathbb{C}$.}}

Note 50

85c981d4f1564164bb547096829d245b

A finite group is {{c3::abelian}} {{c2::if and only if}} its group table is {{c1:: a symmetric matrix.}}

Note 51

859ef5188ad14b35b58dc9428333e5ad

Let G a group and $x \in G$ and $a, b \in$ {{c2::$\mathbb{Z}$}}. Then $x^{a+b} =$ {{c1::$x^a x^b$}}.

Note 52

0c6c419e61fc48139ff6afd4a8e28be6

Let G a group and $x \in G$. Then $|x^{-1}| =$ {{c1::$|x|$}}.

Note 53

f221410dc76e4c7881175d62226ecdf4

Let G a group and $x, g \in G$. Then $|g^{-1}xg| =$ {{c1::$|x|$}}.

Note 54

9951f3d62ec841df9c6f8cfc07f3c04f

Let G a group and $a, b \in G$. Then $|ba| =$ {{c1::$|ab|$}}.

Note 55

b30a94de99fe4c2f91b5417fdbb3e99d

Let G a group, $x \in G$, $|x| = n < \infty$ and $s \in \mathbb{Z}$. Then {{c3::$x^s = 1$}} {{c2::if and only if}} {{c1::$n \mid s$.}}

Note 56

5a0539b7021242e2a9a5769a1c156889

Let G a group, $x \in G$, $|x| =$ {{c3::$n < \infty$}} and $s \in$ {{c4::$\mathbb{Z}$}}. Then

{{c2::$|x^s|$}} $=$ {{c1:: $\dfrac{n}{(n, s)}$.}}

Note 57

7ec585d338e941d7b465cf11d0f42550

Let G a group, $x \in G, |x| = n < \infty$ and $s \in \mathbb{Z}$. Then $|x^s| = \frac{n}{(n,s)}$. What is the key idea in the proof?

> $(x^s)^k = 1$ if and only if $n \mid sk$.

Note 58

00c58492691e442b9a8c0a5ba21a0c7f

Let G a group, $a \in G$. If $x^2 = 1$ for all $x \in G$ then

$$a^{-1} = \text{\{\{c1::}a.\text{\}\}}$$

Note 59

89199067c84244c094af347afff31c8a

Let G a group. If {{c3::a and b are commuting elements of G}} then {{c2::$(ab)^n$}} $=$ {{c1::$a^n b^n$}}.

Note 60

87374145922242e3a5bc43fa952448dc

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is {{c1::abelian.}}

Note 61

cdf7b8b7731c4e619920d66f7520b423

Let G a group. If $x^2 = 1$ for all $x \in G$ then G is abelian. What is the key idea in the proof?

> $1 = (ab)^2$ and multiply by a on the left and by b on the right.

Note 62

c48695948e6a4cf69846a629c6b45cb5

Let $(G, \star)$ be a group and {{c4::$H \subseteq G$.}} If {{c2::H is a group under the operation $\star$ restricted to H}} then {{c3::H}} is called {{c1::a subgroup of G.}}

Note 63

39703ef9887d48e9b763bea0c6519b19

Let G a group and {{c3::$x \in G$.}} Then {{c2::the subgroup $\{x^n \mid n \in \mathbb{Z}\}$ of G}} is called {{c1::the cyclic subgroup of G generated by x.}}

Note 64

7d1e317bc7c64c538d09a6fd6c2e2011

Let A and B be groups. Then $A \times B$ is {{c3::abelian}} {{c2::if and only if}} {{c1::both A and B are abelian.}}

Note 65

c048d6c9ce83411c94e040e5991b3524

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is {{c1::the least common multiple of $|a|$ and $|b|$.}}

Note 66

de71dcf7adc64bcd9b53502c90a0cefa

Let A and B be groups, $(a, b) \in A \times B$. Then

$$(a, b)^k = \text{\{\{c1::}(a^k, b^k)\text{\}\}}$$

for all $k \in$ {{c2::$\mathbb{Z}$}}.

Note 67

e672cc6907124507a4fd998675844d02

Let A and B be groups, $(a, b) \in A \times B$. Then the order of (a, b) is the least common multiple of $|a|$ and $|b|$. What is the key idea in the proof?

> $(a, b)^k = (a^k, b^k)$.

Note 68

e6f9e981e45d4f55a3aafa3eb6d77ef1

Any finite group of {{c2::even}} order contains an element of order {{c1::2.}}

Note 69

d13862b410194166829309d8ea4880a6

Any finite group of even order contains an element of order 2. What is the key idea in the proof?

> Show that the set $\{g \in G \mid g \neq g^{-1}\}$ has an even number of elements.

Note 70

86e37f9ff199460995332631a61f9a00

Let G a group, $x \in G$ and $|x| = n < \infty$. Then the elements {{c2::

$$1, x, x^2, \ldots, x^{n-1}$$

}} {{c1::are distinct.}}

Note 71

1bf4e9f92f854544bf96f1364e0064ed

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x|${{c2:: $\leq$ }}{{c1:: $|G|$ }}.

Note 72

5f4f77e21f2b4052979906547275dfd9

Let G a group, $x \in G$ and $|x| < \infty$. Then $|x| \leq |G|$. What is the key idea in the proof?

> The elements $1, x, \ldots, x^{n-1}$ are the only powers of x.

Note 73

4f07acc87f6949e092c057cb5a580c77

Let G a group, $x \in G$ and $|x| = \infty$. Then the elements {{c2::

$$x^n, n \in \mathbb{Z}$$

}} {{c1::are distinct.}}